

Application No.: 09/928,491
Old Attorney's Docket No. 027557-061
New Attorney's Docket No. 0119-078
Page 4

REMARKS

Claims 28-39 are now pending in the application. Claims 1-27 have been canceled without prejudice or disclaimer. New claims 28-39 have been amended without introduction of new matter. Favorable reconsideration is respectfully requested in view of the above amendments and the following remarks.

Claims 8, 9, 12-15, and 17 stand rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter.

This rejection has been rendered moot by the cancellation of claims 8, 9, 12-15, and 17, and should therefore be withdrawn.

The new claims 28-39 which are now presented for examination are believed to define statutory subject matter at least because they satisfy the test of defining embodiments that achieve useful, tangible and concrete results, as required under Section 101. The method claims 28-33 define various steps that require interaction with a physical environment, and the apparatus claims 34-39 define embodiments of a mobile communications comprising various physical structures.

Claims 1, 3, 5, and 6 stand rejected under 35 U.S.C. §102(b) as allegedly being anticipated by Caputo et al. (U.S. Patent No. 5,778,071). Claims 2, 4, 8, 9, 12, and 14-27 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Caputo et al. in view of Grimm et al. (U.S. Patent No. 5,907,815) and further in view of Geiger et al. (U.S. Patent No. 6,463,534). Claims 7, 10, and 11 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Caputo et al. Grimm et al., and Geiger et al. and further in view of Ericsson, "Bluetooth – A Global Specification for Wireless Connectivity." Claim 13 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Caputo et al., Grimm et al., and Geiger et al., and further in view of Gullman et al. "Biometric Token For Authorizing Access to a Host System." Claims 1-27 stand rejected under 35 U.S.C. §102(a) as allegedly being unpatentable over Nordman (U.S. Patent No. 6,061,346).

Each of these rejections has been rendered moot by the cancellation of claims 1-27 without prejudice or disclaimer.

New claims 28-39 have been added without introduction of new matter. For example, independent method claim 28 defines a method of operating a mobile communications device that includes a cryptographic module. Apparatus claim 34 similarly defines a mobile

Application No.: 09/928,491
Old Attorney's Docket No. 027557-061
New Attorney's Docket No. 0119-078
Page 5

communications device comprising, *inter alia*, a cryptographic module. The mobile communication device is illustrated in, for example, FIG. 1 (see "WAP-enabled client device 10"). That it includes a cryptographic module is stated at, for example, page 4, line 16.

Independent method claim 28 includes the step of "detecting whether a node accessed by the mobile communications device via a wireless network requires performance of an authentication, and in response to detecting that the node accessed by the mobile communications device via the wireless network requires performance of the authentication, using the cryptographic module to carry out the authentication." Independent apparatus claim 34 similarly defines means for carrying out a comparable function. Support for the device "detecting whether the node accessed by the mobile communications device via a wireless network requires performance of an authentication" may be found at, for example, page 5, lines 30-34. That the mobile communications device, in response to the just-described detection "uses the cryptographic module to carry out the authentication" is described at, for example, page 4, lines 15-20.

Independent method claim 28 includes the additional step of "detecting whether a local external device having a connection to a network by means other than the mobile communications device requires performance of an authentication, and in response to detecting that the local external device requires performance of the authentication, using the cryptographic module to carry out the authentication." Independent apparatus claim 34 similarly defines means for carrying out a comparable function. Support for the local external device "having a connection to a network by means other than the mobile communications device" may be found in, for example, FIG. 1, which illustrates the PC 60 having its own connection to a modem 56, independent of the mobile communications device 10. Support for the mobile communications device "detecting whether a local external device ... requires performance of an authentication" may be found at, for example, the text spanning page 9, line 27 through page 10, line 15, which not only describes the mobile communications device 10 operating in support of a local external device (e.g., the personal computer 60), but also describes both automatic and manual methods of starting this particular functionality (e.g., the use of commands using the AT protocol when there is a connection between the mobile device 10 and the personal computer 60, and the use of a specific key press on the keyboard of the phone when there is no connection between the mobile device 10 and the personal computer 60). Those of ordinary skill in the relevant art

Application No.: 09/928,491
Old Attorney's Docket No. 027557-061
New Attorney's Docket No. 0119-078
Page 6

would readily understand that it is inherent that the device would be able to "detect" the commands (e.g., in accordance with the AT protocol, or the key depressions) calling for the performance of the authentication.

That the mobile communications device, in response to the just-described detection "uses the cryptographic module to carry out the authentication" may be found at, for example, page 8, lines 30-35.

The new dependent claims 29-33 and 35-39 similarly define subject matter that is well-supported by both the original specification and claims.

Embodiments defined by independent claims 28 and 34 are believed to be patentably distinguishable over the prior art of record because they enable a single mobile communications device to achieve a unique efficiency in that a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the authentication requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1.

The Caputo et al. patent fails to disclose the combination of features defined by either of independent claims 28 and 34 for a number of reasons. To begin with, the device disclosed by Caputo et al. is not capable of accessing a node "via a wireless network", as required by the claims. Instead, the Caputo et al. device requires a wired connection to a network. (See, e.g., Fig. 2 and column 5, lines 62-65: "Further, the connector port 14 is a modular receptacle which may be directly connected to a data transfer path, such as a telephone system.") Furthermore, the external device of Caputo et al. does not "hav[e] a connection to a network by means other than the mobile communications device", as required by the claims; instead, Caputo et al.'s computer is connected to the network *through* the device 10 (see, e.g., Caputo et al.'s figure 2). Moreover, the device of Caputo et al. appears to operate in only one mode, namely, for the benefit of the external device (computer); it sits in-between the computer and the network, passing data from one to the other, and performs authentication as required by the node that the *computer* is connected to. Consequently, there is no dual mechanism for both carrying out authentication if "the node accessed by the mobile communications device via the wireless network requires performance of the authentication", and also carrying out the authentication if "the local external device requires performance of the authentication", as required by each of Applicant's independent claims.

Application No.: 09/928,491
Old Attorney's Docket No. 027557-061
New Attorney's Docket No. 0119-078
Page 7

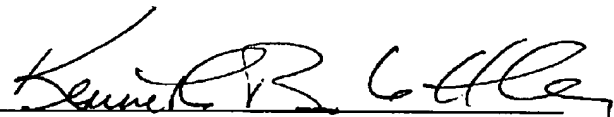
Neither of the Grimm et al. and Geiger et al. patents makes up for the deficiencies of Caputo et al. at least because they each fail to disclose an arrangement whereby a mobile communications device is capable of performing authentication for its own connection to a node via a wireless network, *and also* performing authentication for an external device "having a connection to a network by means other than the mobile communications device," as required by the claims. The Nordman patent, which was also cited against the original claims, is similarly deficient in this regard since the illustrated "wireless host 32" is not described or illustrated as having its own connection to a network by means other than the illustrated GSM mobile terminal 16. Consequently, there would be no motivation for configuring the mobile terminal with a mechanism for providing both modes of operation as defined in Applicant's claims.

For at least the foregoing reasons, the new independent claims 28 and 34, as well as their respective dependent claims 29-33 and 35-39, are believed to be patentable over the prior art of record.

The application is believed to be in condition for allowance. Prompt notice of same is respectfully requested.

Respectfully submitted,
Potomac Patent Group PLLC

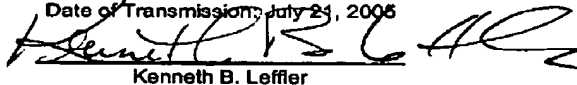
Date: July 21, 2005

By: 
Kenneth B. Leffler
Registration No. 36,075

P.O. Box 855
McLean, Virginia 22101-0855
703-718-8884

I hereby certify that this correspondence is being sent by facsimile transmission to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 to the following facsimile number:

Facsimile Number: 703 872 9308
Date of Transmission: July 24, 2005


Kenneth B. Leffler